iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** V **Month of publication:** May 2018

DOI: http://doi.org/10.22214/ijraset.2018.5265

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue V, May 2018- Available at www.ijraset.com

Improved AES Algorithm for Secure Communication in Cloud

Abhipray Bajpai[1], Dr. D. K. Mishra[2]
[1]*MTECH-Research Scholar Sri Aurobindo Institute of Technology, Indore*
[2]*Professor Sri Aurobindo Institute of Technology, Indore*

Abstract: Cloud Computing provides the facility of shared environment due to its distributed resource nature and open environment. Thus, access of resource is easy from anywhere. Privacy and security are also important at the same time. Computing resources are another demand which makes outsourcing of data by the organizations, which need secure storage in cloud. This paper address secure data storage using AES (Advance Encryption Standard) for increase in confidentiality and security by splitting data files into chunks and then calculating number of keys. In the proposed approach chunk file is formed which generate key and then encryption on chunk file is performed. The proposed model uses count to generate multiple numbers of keys

Keywords: Key generation; AES; chunk file; encryption; Decryption; count

I. INTRODUCTION

According to NIST, cloud is defined as the model which is convenient to serve with on-demand services and resources with decreased cost and easy to access service. Cloud environment is fully configured but require internet connection for accessing resources and services. Cloud is a pool of resources which is the combination of distributed and shared computing offering beneficial aspects of software and hardware services. It is a cost effective service which is integrated with service model and has the ability to cope with the change in trend. Cloud computing serves with storage, server, network and a complete infrastructure to access applications and software easily. In this approach improved AES algorithm is used and this algorithm works on single key i.e, Symmetric key algorithm, with encrypt and decrypt data with processing of large data. But in terms of computation it is not so intensive which leads to less overheads on system with high performance of encryption and decryption speed. Symmetric algorithms encrypt plaintext bit by bit as a stream cipher or encrypt plaintext with fixed number of 64 units as a Block cipher.

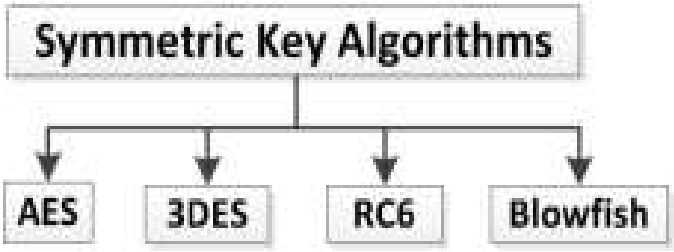


Figure 1: Symmetric Algorithms

A. Security In Cloud Computing

In terms of data storage on cloud, public storage is not costly but is not secure. Different models provide different services and requirements inrease on the basis of internal cost and performance. To preserve data, effective technologies are required, which protect, manage and assure security of data.

B. Some steps are Involved for The Secure Cloud Storage Areas

More efficiency is required in cloud for adapting storage-as-a-service. Mitigation approach is required to reduce risk of data in cloud service by improving services. Complete life cycle of data is managed by SLA, Service Level Agreement BNo investment is required for accessing of data and storage of data on cloud. Requirements are flexible and can be modified and enabled.

II. RELATED WORK

A. Study of Existing Work With Diagram

Babitha. M.P et al. In[1] In existing work, security issues are evaluated by proposing security method for cloud data. AES is used which works for 128 bit key size to serve with access control, confidentiality and authenticity. After it, performance on the basis of delay is analyzed using approach used by author. This analysis describes the increase in delay in file size. Different types of security issues and privacy protection issues are addressed in cloud with providing security services like authorization, authentication and confidentiality by monitoring delay.

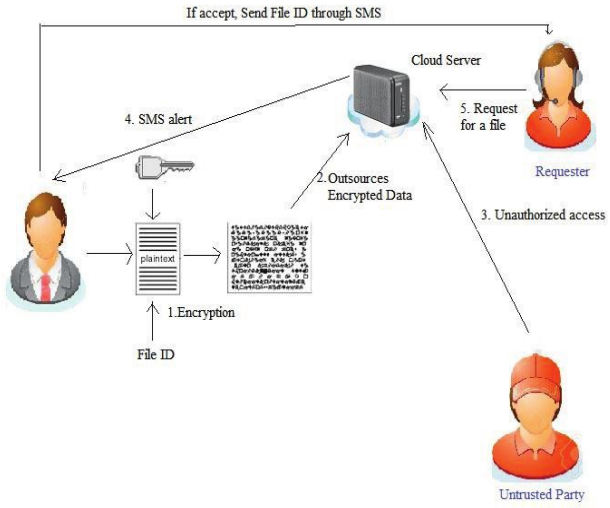


Figure 2: System architecture of existing work [1]

Table 1. Comparative Table

AUTHOR	TITLE	PROPOSED WORK
Hyun-Suk Yu, Yvette E. Gelogo, K J Kim [2]	Securing Data Storage in Cloud Computing	Author also recommended an integrated model for security in cloud infrastructure. Also proposed a security mechanism for secure data storage.
C.W. Hsu, C.W. Wang, Shiuhpyng Shieh [3]	Reliability and Security of Large Scale Data Storage in Cloud Computing	Observe the important characteristics like distributed capabilities for storage and security using CAP theorem.
Qian Wang, Cong Wang, Jin Li, Kui Ren, Wenjing Lou [4]	Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing	implemented the issue of data integrity in cloud computing. A third party auditor is used for the verification of integrity in dynamic data Which improves the retrievability model using hash tree for authentication.
P. Mell, Grance [5]	The NIST definition of cloud computing	Proposed about model which integrate technologies like web services, service level agreement (SLA) and virtualization for application enterprises. t

III. PROBLEM DOMAIN

Existing system used AES for the encryption of data in cloud. Data stored in cloud is firstly encrypted using Advanced Encryption Standard, but issue arises in existing system is the symmetric key. AES is a symmetric key algorithm which suffers with key

compromising issue and this issue leads to access of data by intruders and attackers. Victim may loss data confidentiality and privacy due to fabrication of message.

A. Key compromising may lead to

1) *Data confidentiality:* Data confidentiality and privacy may loss due to attack.
2) *Integrity:* Unauthorized access reduces accuracy of data.
3) *Availability:* Data availability may be affected lead to denial of services

IV. SOLUTION DOMAIN

To address the above problem proposed system will be implemented, which is also working on the AES technique but improved this technique using multi key generation. Data is encrypted using AES technique and the generated key by converting data into cipher text. N is the number of keys are calculated using count which solves the issue of key compromising. In the proposed approach chunk file is formed which generate key and then encryption on chunk file is performed. The proposed model uses count to generate multiple numbers of keys.

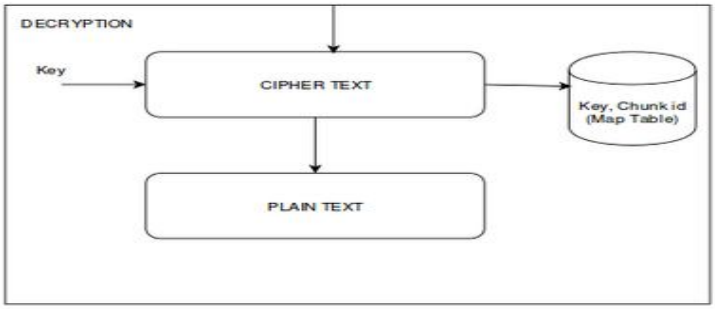


Figure 3. System Architecture for encryption

V. RESULT ANALYSIS

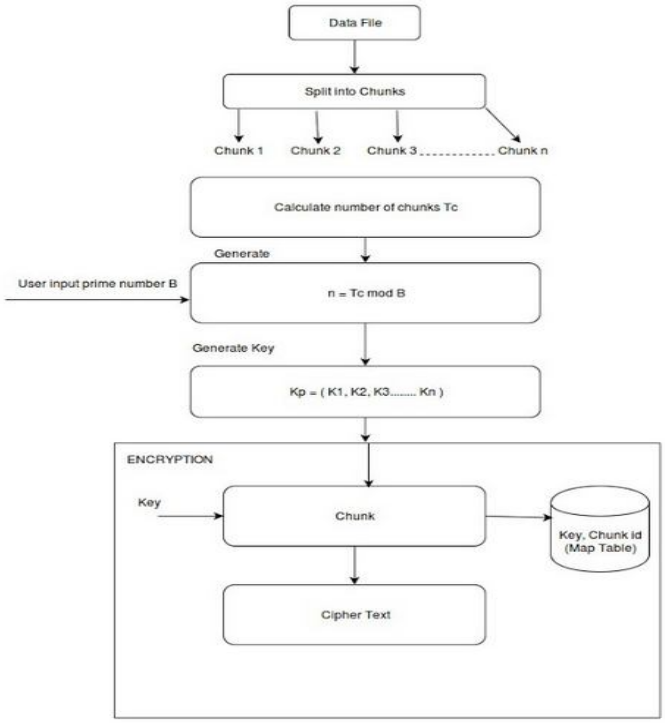


Figure 4: System Architecture for decryption

VI. CONCLUSION

Privacy and security are also important at the same time which need secure storage in cloud. This paper address secure data storage using AES (Advance Encryption Standard) for increase in confidentiality and security by splitting data files into chunks and then calculating number of keys. The proposed model uses count to generate multiple number of keys after it encryption on data is performed.

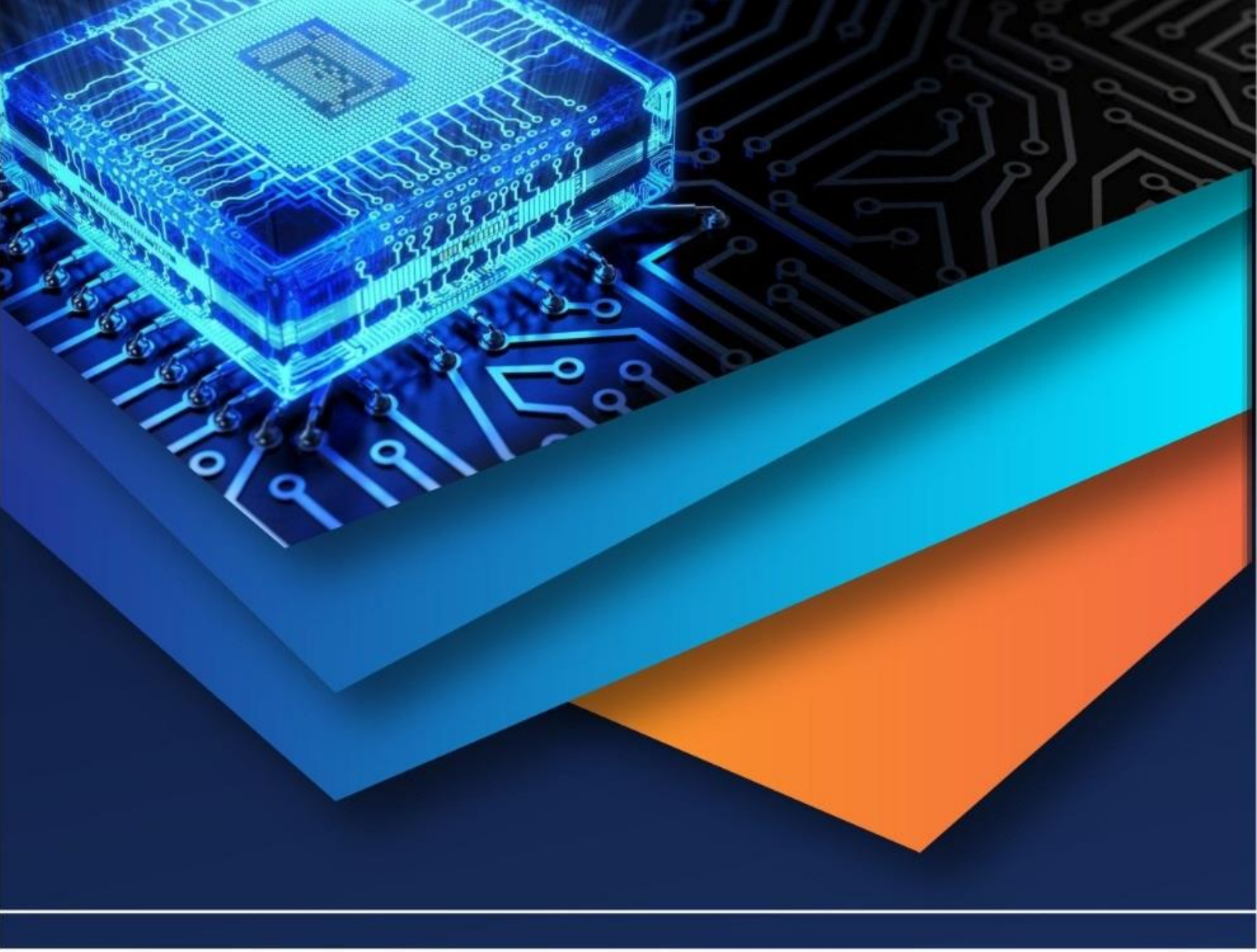
A. An improved AES algorithm is used in our work with multi key AES.
B. MD5 is used to achieve authentication.
C. It generate key and then encryption on chunk file is performed.
D. N number of keys is calculated using count which solves the issue of key compromising.

VII.FUTURE WORK

In future implementation modified AES can be replaced by Blowfish algorithm for better performance.
Strong Authentication can be implemented in future scope.
Image data can also be implemented in future work.

REFERENCES

[1] Babitha.M.P, K.R. Remesh Babu, “Secure Cloud Storage Using AES Encryption,” 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT), IEEE.
[2] Hyun-Suk Yu, Yvette E. Gelogo, K J Kim, “Securing Data Storage in Cloud Computing”, J. of Security Engineering, June 2012, pp.252-259.
[3] C.W. Hsu, C.W. Wang, Shiuhpyng Shieh, “Reliability and Security of Large Scale Data Storage in Cloud Computing”, part of the Reliability Society Annual Technical Report 2010.
[4] Qian Wang, Cong Wang, Jin Li, Kui Ren, Wenjing Lou, “Enabling Public Verifiability and Data Dynamics for Storage Security in Cloud Computing”, IEEE Systems Journal, Vol.9, No.1, August 2015.
[5] P. Mell, Grance, “The NIST definition of cloud computing”, Natl. Inst. Standards Technol.(NIST), U.S. Dept. of Commerce, Gaithersburg, MD, USA, NIST Special Publication; Sep.2011, pp. 800-145.
[6] S. Subashini, V. Kavitha, “A survey on security issues in service delivery models of cloud computing”, Journal of Network and Computer Applications, Vol. 34, Iss. 1, Jan 2011, pp.1–11.
[7] Paul C. H., S Rao, C B. Silio, A Narayan, “System of Systems for Quality-of-Service Observation and Response inCloud Computing Environments”, IEEE Systems Journal. Vol.9, No.1, March 2015, pp. 212-222.
[8] D Ardagna, G Casale, M Ciavotta, J F Perez, W Wang, "Quality-of-service in cloud computing: modeling techniques and their applications", Journal of Internet Services and Applications, 5:11, 2014, pp. 1-17.
[9] S.Lee, D.Tang, T.Chen, W.C.Chu, “A QoS assurance middleware model for enterprise cloud computing”, IEEE 36 th Int. Conf. on Computer Software and Application Workshops, 2012, pp. 322-327.
[10] Vipul Goyal, Omkant Pandey, Amit Sahai, Brent Waters ,“Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data”, ACM Conference on Computer and Communication (CCS 2006), pp. 89-98.
[11] Leena Khanna, Anant Jaiswal, “Cloud Computing: Security Issues and Description of Encryption Based Algorithms to Overcome Them”, IJARCSSE 2013
[12] Nelson Gonzalez, Charles Miers, Fernando Redigolo, Marcos Simplicio, Tereza Carvalho, Mats Naslund, Makan Pourzandi “A quantitative analysis of current security concerns and solutions for cloud computing”, Springer 2012.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY